Error-Correction Capability of Reed-Muller codes

Stéphanie Dib, François Rodier

Error-Correction Capability of Reed-Muller codes

Stéphanie Dib, François Rodier *

Abstract

We present an asymptotic limit between correctable and uncorrectable errors on the Reed-Muller codes of any order. This limit is theoretical and does not depend of any decoding algorithm.

1 Introduction

Let $\mathbb{F}_2$ be the field with 2 elements, and let $RM = RM(n, r)$ be the Reed-Muller code of length 2^n and of order r that is the set of Boolean function with n variables of algebraic degree not more than r.

Building a code is important, but we must think about how many words we can decode. Usually, we content ourselves of the fact that errors of weights less than half of the minimum distance can be corrected in a unique manner. So decoding an error correcting code beyond half of the minimum distance has been a challenge for the one who study error correcting codes. In fact experiments show that a maximum likelihood decoding can decode many more words.

Here we propose a theoretical bound for decoding almost all errors of Reed-Muller code on any order by this method of decoding. Indeed, the decoder will often be able to recover the correct codeword using an algorithm that generates for each received word the closest codeword even if the received word is more distant than half of the minimum distance. On the contrary, when the number of errors exceeds a certain value, the received vector will be rarely closer to the correct codeword than to any other one. Here we give a proof for that.

*Aix Marseille Université, CNRS, Centrale Marseille, Institut de Mathématiques de Marseille, UMR 7373, 13288 Marseille, France, stephania.dib@gmail.com, francois.rodier@univ-amu.fr

It is interesting to compare that fact with the phenomenon of concentration of the nonlinearity of Boolean functions which have been studied by several authors ([3, 4, 9, 11, 12, 13]. The r-nonlinearity of a Boolean function f denoted $NL_r(f)$ is its Hamming distance to the set of Boolean functions with n variables of algebraic degree not more than r. Claude Carlet [2], proved that the density of the set of Boolean functions satisfying

$$NL_r(f) > 2^{n-1} - c\sqrt{2^{n-1}\binom{n}{r}\log 2}$$

tends to 1 when n tends to infinity, if $c > 1$. The authors of the present paper proved a concentration of the nonlinearities of almost all Boolean functions around

$$2^{n-1} - \sqrt{2^{n-1}\binom{n}{r}\log 2} \tag{1}$$

when $r \leq 2$ but missed the greater values by lack of knowledge of weight distributions ([3, 4, 11, 12]. Kai-Uwe Schmidt generalized this result for all r thanks to a result of Kaufman, Lovett, and Porat [8] helping him to find a better bound for the weights of a RM code [13].

On the other hand, Helleseth, Klove and Levenshtein in the paper *Error correction capability of binary linear codes* [7] study order 1 or 2 Reed-Muller codes and they show that almost all the words are decodable up to the same bound as (1) and almost all words are not decodable beyond this bound. For that, they use the monotone structure of correctable and uncorrectable errors. Stéphanie Dib [4, Chapter 3] proved by the same method as for the concentration of the nonlinearities of almost all Boolean functions that the bound for correcting most of the values of codewords for 1-order RM codes was given by (1).

We show here that the value given in (1) is also the bound for correcting most of the values of codewords for RM codes for any order. For RM codes, the present work improves the paper by Helleseth et al. [7] where they just prove the fact that the codes $RM(n, r)$ are asymptotically optimal for $r = 1$ (cf. note after inequality (54) of [7]) or $r = 2$ (example 7 of [7]).

2 Presentation

Let $d(e, f)$ be the Hamming distance between the elements e and f in $\mathbb{F}_2^{2^n}$. We denote by $wt(e)$ the weight of an element e in $\mathbb{F}_2^{2^n}$. Let C be a linear code of length m, of dimension k. The Reed-Muller code of length 2^n and of order r has dimension $\sum_0^r \binom{n}{r}$ and minimum distance 2^{n-r}.

2.1 Correctable and uncorrectable errors

Let $\mathbb{F}_2^{2^n}$ be the set of all binary vectors of length 2^n. For any vector $f \in \mathbb{F}_2^{2^n}$, the set

$$f + C = \{f + g \mid g \in C\}$$

is called a coset of C and contains 2^k vectors. One can easily check that two cosets are either disjoint or coincide. This means

$$f \in h + C \Longrightarrow f + C = h + C.$$

Therefore, the set $\mathbb{F}_2^{2^n}$ can be partitioned into 2^{2^n-k} cosets of C:

$$\mathbb{F}_2^{2^n} = \bigcup_{i=0}^{2^{2^n-k}-1} (f_i + C), \qquad f_i \in \mathbb{F}_2^{2^n}$$

where $(f_i + C) \cap (f_j + C) = \emptyset$ for $i \neq j$.
If you send a word g and the decoder receive the word h, we will call $e = g - h$ the error. Thus, the possible error vectors are the vectors in the coset containing h. In maximum-likelihood decoding, the decoder's strategy is, given h, to choose a minimum weight vector e in $h + C$, and to decode h as $h - e$.
The minimum weight vector in a coset is called the coset leader, and when there is more than one vector of minimum weight in a coset, any one of them can be selected as the coset leader.
We denote the set of all coset leaders by $E_0(C)$ (note that $\#E_0(C) = 2^{2^n-k}$). The elements of $E_0(C)$ are called correctable errors, and the elements of $E_1(C) = \mathbb{F}_2^n - E_0(C)$ are called uncorrectable errors. Only coset leaders are correctable errors, which means that 2^{2^n-k} errors can be corrected with this decoding.
A codeword is an unambiguous correctable error if it is a coset leader, and it is the only vector of minimum weight in this coset.

Proposition 1 .
The following statements are equivalent.

1- *A codeword e is an unambiguous correctable error;*

2- $\forall e' \in e + C$ *if* $e \neq e'$ *then* $wt(e) < wt(e')$*;*

3- $\forall g \in C - \{0\},\ wt(e) < wt(g + e)$*;*

4- $\forall g \in C - \{0\},\ d(e, 0) < d(g, e)$.

Proof
The first assertion implies the second because if $e' \in e + C$ and $e \neq e'$ then e' is not the coset leader, so $wt(e) < wt(e')$.
The second assertion implies the first because if $e' \in e + C$ and $e \neq e'$ then $wt(e) < wt(e')$ so e' is not the coset leader and e is the only vector of minimum weight in this coset.
The other statement are clear.

2.2 The probability

We take $\mathbb{F}_2^{2^n}$ as the probability space. We endow it with the uniform probability P.

3 The results

Let $\lambda_n = c \times 2^{n/2}\sqrt{2\binom{n}{r}\log 2}$ and $\delta = 2^{n-1} - \lambda_n/2$ where c is a positive real.

We will show that if $c > 1$ then almost all error of weight smaller than δ are correctable, when n tends to infinity. And that if $c < 1$ then almost all error of weight higher than δ are uncorrectable, when n tends to infinity. More precisely we will show the following two theorems.

Theorem 1 . *Let $c > 1$. Then*

$$P_{wt(e)\leq\delta}\Big(d(e,0) < d(e,g) \text{ for all } g \in RM(r) - 0\Big) \to 1 \text{ when } n \to \infty.$$

and

Theorem 2 . *Let $c < 1$. Then*

$$P_{wt(e)\geq\delta}\Big(\text{there exists } g \in RM(r) - 0 \text{ such that } d(e,0) \geq d(e,g)\Big) \to 1 \text{ when } n \to \infty.$$

4 Proof of the Theorem 1. Decoding a large number of errors

We intend to prove that almost all error of weight smaller than δ for $c > 1$ are correctable, when n tends to infinity. It is enough to prove

$$P_{wt(e)\leq\delta}\Big(d(e,0) < d(e,g) \text{ for all } g \in RM(r) - 0\Big) \to 1 \text{ when } n \to \infty.$$

We have just to show

$$P_{wt(e)\leq\delta}\Big(\delta < d(e,g) \text{ for all } g \in RM(r) - 0\Big) \to 1 \text{ when } n \to \infty$$

or

$$P_{wt(e)\leq\delta}\Big(\exists g \in RM(r) - 0,\ \delta \geq d(e,g)\Big) \to 0 \text{ when } n \to \infty$$

that is

$$P_{wt(e)\leq\delta}\left(\bigcup_{g\in RM(r)-0}\Big(\delta \geq d(e,g)\Big)\right) \to 0 \text{ when } n \to \infty.$$

It is enough to prove that

$$\sum_{g\in RM(r)-0} P_{wt(e)\leq\delta}\left(\delta \geq d(e,g)\right) \to 0 \text{ when } n \to \infty.$$

By expressing the conditional probabilities we have to show that

$$\sum_{g\in RM(r)-0} \frac{P\Big(\Big(d(e,0) \leq \delta\Big) \cap \Big(d(e,g) \leq \delta\Big)\Big)}{P\Big(d(e,0) \leq \delta\Big)} \to 0 \text{ when } n \to \infty.$$

Let $B_\delta(g)$ be the ball of center g and of radius δ that is the set of e such that $d(e,g) \leq \delta$. The event $B_\delta(g)$ is the set of words f in $\mathbb{F}_2^{2^n}$ such $f \in B_\delta(g)$, that is $d(f,g) \leq \delta$.

Hence Theorem 1 is a consequence of the following proposition.

Proposition 2 . *If $c > 1$ then*

$$\sum_{g\in RM(r)-0} \frac{P\Big(B_\delta(0) \cap B_\delta(g)\Big)}{P\left(B_\delta(0)\right)} \to 0 \text{ when } n \to \infty$$

Before the proof of this Proposition we have to evaluate the terms in the sum.

Lemma 1 . *For every real s, one has*

$$P\Big(B_\delta(0) \cap B_\delta(g)\Big) \ \leq\ \exp\Big(2s^2(2^n - wt(g)) - 2s\lambda\Big).$$

Proof.
Replace δ by its value.

$$\begin{aligned} P\Big(B_\delta(0) \cap B_\delta(g)\Big) &= P\Big(\left(wt(f) \leq \delta\right) \cap \left(wt(f+g) \leq \delta\right)\Big) \\ &= P\Big((2^{n-1} - wt(f) \geq \lambda/2) \cap (2^{n-1} - wt(f+g) \geq \lambda/2)\Big) \end{aligned}$$

One knows that

$$2^n - 2wt(f) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)}, \quad 2^n - 2wt(f+g) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+g(x)}.$$

Hence this gives using Markov's inequality:

$$\begin{aligned}
&P\Big(B_\delta(0)\cap B_\delta(g)\Big)\\
&\quad= P\left(\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)}\geq\lambda\right)\cap\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+g(x)}\geq\lambda\right)\right)\\
&\quad= P\left(\left(\exp\left(s\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)}\right)\geq\exp(s\lambda)\right)\cap\right.\\
&\qquad\qquad\left.\left(\exp\left(s\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+g(x)}\right)\geq\exp(s\lambda)\right)\right)\\
&\quad\leq E\left(\exp\Big(s\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)}\Big)\exp\Big(s\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+g(x)}\Big)\right)\Big/\exp(s\lambda)^2
\end{aligned}$$

Since the random values $f(x)$ are independant

$$\begin{aligned}
P\Big(B_\delta(0)\cap B_\delta(g)\Big) &\leq E\left(\exp\Big(\sum_{x\in\mathbb{F}_2^n} s(-1)^{f(x)}\Big(1+(-1)^{g(x)}\Big)\Big)\right)\Big/\exp(s\lambda)^2\\
&\leq \prod_{x\in\mathbb{F}_2^n} E\left(\exp\Big(s(-1)^{f(x)}\Big(1+(-1)^{g(x)}\Big)\Big)\right)\Big/\exp(s\lambda)^2
\end{aligned}$$

Because the random values $f(x)$ takes the values ±1 with probability $1/2$, the calculation of the expectation gives

$$P\Big(B_\delta(0)\cap B_\delta(g)\Big) \leq \prod_{x\in\mathbb{F}_2^n}\cosh\Big(s\Big(1+(-1)^{g(x)}\Big)\Big)\Big/\exp(s\lambda)^2$$

As $\cosh(t)\leq\exp(t^2/2)$

$$\begin{aligned}
P\Big(B_\delta(0)\cap B_\delta(g)\Big) &\leq \prod_{x\in\mathbb{F}_2^n}\exp\Big(s^2\Big(1+(-1)^{g(x)}\Big)^2/2\Big)\Big/\exp(s\lambda)^2\\
&\leq \exp\left(s^2\Big(2^n+\sum_{\mathbb{F}_2^n}(-1)^{g(x)}\Big)\right)\Big/\exp(s\lambda)^2\\
&\leq \exp\Big(2s^2(2^n-wt(g))-2s\lambda\Big).
\end{aligned}$$

4.1 Case where the distances are close to 2^{n-1}.

We give a bound for $P\Big(B_\delta(0) \cap B_\delta(g)\Big)$ when the distance to 0 of the center g is rather close to 2^{n-1}.

Lemma 2 . *If*

$$|2^{n-1} - d(g,0)| \leq 2^{n-1} / \binom{n}{r}$$

then:

$$P\Big(B_\delta(0) \cap B_\delta(g)\Big) \;\leq\; \frac{1}{2^{c^2 2\left(\binom{n}{r}-1\right)}}.$$

Proof.
From lemma 1 we have

$$\begin{aligned} P\Big(B_\delta(0) \cap B_\delta(g)\Big) &\leq \exp\Big(s^2\Big(2^n + 2^n - 2wt(g)\Big)\Big) \Big/ \exp(s\lambda)^2 \\ &\leq \exp\Big(s^2 2^n\Big(1 + 1\Big/\binom{n}{r}\Big)\Big) \Big/ \exp(s\lambda)^2 \end{aligned}$$

We take $s = \lambda/2^n$.

$$\begin{aligned} P\Big(B_\delta(0) \cap B_\delta(g)\Big) &\leq \exp\Big(\lambda^2 2^{-n}\Big(1 + 1\Big/\binom{n}{r}\Big)\Big) \Big/ \exp(\lambda^2/2^{n-1}) \\ &\leq \exp\Big(2c^2\binom{n}{r}\log 2\Big(1 + 1\Big/\binom{n}{r}\Big)\Big) \Big/ \exp\Big(4c^2\binom{n}{r}\log 2\Big) \end{aligned}$$

Simplifying the two members of this fraction by $\exp\Big(2c^2\binom{n}{r}\log 2\Big)$ you get

$$P\Big(B_\delta(0) \cap B_\delta(g)\Big) \;\leq\; \frac{\exp\left(2c^2 \log 2\right)}{\exp(2c^2\binom{n}{r}\log 2)} \leq \frac{2^{2c^2}}{2^{c^2 \times 2\binom{n}{r}}}$$

4.2 Case where the distances are away from 2^{n-1}.

We use the follwing lemma, which is an application of a result by Kaufman, Lovett, and Porat [8].

Lemma 3 . *Let α be a strictly positive real number. The number $B_{r,n}$ of functions g in $RM(r,n)$ satisfying*

$$|wt(g) - 2^{n-1}| \geq 2^{n-1} / \binom{n}{r}$$

fulfills

$$B_{r,n} \leq 2^{\alpha\binom{n}{r}}$$

if n is large enough.

Proof
This is shown in the proof of Lemma 3 in K.-U. Schmidt's article [13, relation (6)].

We use this lemma to evaluate $\Pi = \sum P\Big(B_\delta(0) \cap B_\delta(g)\Big)$ where the sum is on the nonzero g in $RM(n,r)$ fulfilling

$$|wt(g) - 2^{n-1}| \geq 2^{n-1} \Big/ \binom{n}{r}.$$

Lemma 4 . *Let α be a strictly positive real number. Then*

$$\Pi < 2^{\alpha\binom{n}{r}} 2^{-\frac{c^2}{1-2^{-r}}\binom{n}{r}}$$

Proof.
From lemma 1, for all s, we have

$$P\Big(B_\delta(0) \cap B_\delta(g)\Big) \leq \exp\Big(2s^2(2^n - wt(g)) - 2s\lambda\Big)$$

Let us take $s = \dfrac{\lambda}{2^{n+1} - 2wt(g)}$. We have, expressing the value of λ and noting that $wt(g)$ is not less than the minimum distance 2^{n-r} of $RM(n,r)$:

$$\begin{aligned} P\Big(B_\delta(0) \cap B_\delta(g)\Big) &\leq \exp\left(-\frac{\lambda^2}{2^{n+1} - 2wt(g)}\right) \\ &\leq \exp\left(-\frac{c^2 \times 2^{n+1}\binom{n}{r}\log 2}{2^{n+1} - 2^{n-r+1}}\right) \\ &\leq 2^{-\frac{c^2 \times \binom{n}{r}}{1-2^{-r}}}. \end{aligned}$$

Therefore

$$\Pi \leq B_{r,n} 2^{-\frac{c^2}{1-2^{-r}}\binom{n}{r}} \leq 2^{\alpha\binom{n}{r}} 2^{-\frac{c^2}{1-2^{-r}}\binom{n}{r}}.$$

4.3 Evaluation of $P\left(B_\delta(0)\right)$

Proposition 3 . *Let r be a fixed integer, $\delta = 2^{n-1} - c\sqrt{2^{n-1}\binom{n}{r}\log 2}$ where c is a positive constant. We have*

$$P\left(B_\delta(0)\right) = \frac{1}{2\pi} \frac{2^{-c^2\binom{n}{r}}}{2c\sqrt{\binom{n}{r}\log 2}}(1 + o(1)) \tag{2}$$

when n tends to infinity.

This is proved in Stéphanie Dib's thesis [4]. We recall briefly the proof for completeness.
The following lemma (see [2, lemma 1]) gives well-known asymptotic estimate of the sum of binomial coefficients.

Lemma 5 . *Let n be a positive integer and $k \leq n$. Then*

$$\sum_{i=0}^{k} \binom{2n}{i} < 2^{2n} \cdot \exp\left(-\frac{(n-k)^2}{n}\right).$$

When k is sufficiently close to n, the following lemma (see [6, chapter IX, (9.98)], [5, chapter VII]) gives an asymptotic estimation for $\binom{2n}{k}$:

Lemma 6 . *Let n be a positive integer and $|n-k| \leq n^{\frac{5}{8}}$. Then*

$$\binom{2n}{k} = \frac{2^{2n}}{\sqrt{\pi \cdot n}} \cdot \exp\left(-\frac{(n-k)^2}{n}\right) \cdot (1 + o(1)), \tag{3}$$

where the term $o(1)$ is independent of the choice of k.

Proof of the Proposition.
The number of Boolean functions whose Hamming distance to 0 is bounded from above by some number δ equals $\sum_{0 \leq i \leq \delta} \binom{2^n}{i}$. Thus we have

$$\sum_{0 \leq i \leq \delta} \binom{2^n}{i} = \sum_{0 \leq i < 2^{n-1} - 2^{(n-1)\frac{5}{8}}} \binom{2^n}{i} + \sum_{2^{n-1} - 2^{(n-1)\frac{5}{8}} \leq i \leq \delta} \binom{2^n}{i}.$$

The first sum on the right hand side is taken care of by lemma 5 which will show that it is negligible with respect of the second sum.
To estimate a lower bound of the second sum (which we denote S), we use (3)

$$S = \frac{2^{2^n}}{\sqrt{\pi\, 2^{n-1}}} \cdot (1 + o(1)) \cdot \sum_{2^{n-1} - 2^{(n-1)\frac{5}{8}} \leq i \leq \delta} \exp\left(-\frac{(2^{n-1} - i)^2}{2^{n-1}}\right).$$

We use that the function in the sum is monotonous to replace the sum by an integral.

$$\begin{aligned} S &= \frac{2^{2^n}}{\sqrt{\pi\, 2^{n-1}}} \cdot (1 + o(1)) \cdot \int_{2^{n-1} - 2^{(n-1)\frac{5}{8}} + 1 \leq i \leq \delta} \exp\left(-\frac{(2^{n-1} - i)^2}{2^{n-1}}\right) di. \\ &= \frac{2^{2^n}}{\sqrt{\pi}} \cdot (1 + o(1)) \cdot \int_{c \sqrt{\binom{n}{r} \log 2} \leq v \leq 2^{\frac{n-1}{8}} - 2^{\frac{1-n}{2}}} \exp\left(-v^2\right) dv. \end{aligned}$$

By [5, chapter VII, Lemma 2] and the fact that

$$c^2\binom{n}{r}\log 2 - \left(2^{\frac{n-1}{8}} - 2^{\frac{1-n}{2}}\right)^2 \to -\infty$$

which implies that

$$\int_{2^{\frac{n-1}{8}}-2^{\frac{1-n}{2}}}^{\infty} \exp\left(-v^2\right) dv = o\left(\int_c^{\infty} \sqrt{\binom{n}{r}\log 2}\exp\left(-v^2\right) dv\right)$$

the last integral is equivalent to

$$\frac{\exp\left(-c^2\binom{n}{r}\log 2\right)}{2c\sqrt{\binom{n}{r}\log 2}} = \frac{2^{-c^2\binom{n}{r}}}{2c\sqrt{\binom{n}{r}\log 2}}.$$

Thus

$$\sum_{0\le i\le\delta}\binom{2^n}{i} = \frac{2^{2^n}}{\sqrt{\pi}}\frac{2^{-c^2\binom{n}{r}}}{2c\sqrt{\binom{n}{r}\log 2}}(1+o(1)).$$

4.4 Proof of Theorem 1

Therefore

$$\sum_{g\in RM(r)-0}\frac{P\Big(B_\delta(0)\cap B_\delta(g)\Big)}{P\left(B_\delta(0)\right)}$$
$$\le O(n^{r/2})\left(2^{\binom{n}{r}}2^{-c^2 2\left(\binom{n}{r}-1\right)}2^{c^2\binom{n}{r}} + 2^{\alpha\binom{n}{r}}2^{-\frac{c^2}{1-2^{-r}}\binom{n}{r}}2^{c^2\binom{n}{r}}\right).$$

This tends to 0 because the exponent of 2 is, for the left term

$$\binom{n}{r} - c^2 2\left(\binom{n}{r}-1\right) + c^2\binom{n}{r} = -\binom{n}{r}c^2 + 2c^2 \to -\infty$$

and for the right term

$$\alpha\binom{n}{r} - \frac{c^2}{1-2^{-r}}\binom{n}{r} + c^2\binom{n}{r} = \binom{n}{r}\left(\alpha - \frac{2^{-r}c^2}{1-2^{-r}}\right).$$

So just take

$$\alpha < \frac{2^{-r}c^2}{1-2^{-r}}$$

so that this term tends to $-\infty$.

5 The error correction capability function

Let $\epsilon_C(t)$ the ratio of the number of correctables errors of weight t to the number of words of weight t. Let us suppose from now on that the lexicographically smallest minimum-weight vectors are chosen as the coset leaders. This involves only the cosets with several minimum weight vectors that is the ambiguous correctable errors. Then an important property of this ratio is that for any t in the range from half the minimum distance to the covering radius, $\epsilon_C(t)$ decreases with the growing t as the next lemma says.

Lemma 7 .
For any $[n, k]$ code C and any $t = 0, 1, \ldots, n-1$

$$\epsilon_C(t+1) \leq \epsilon_C(t)$$

with strict inequality for $t_C \leq t \leq r_C$ where we set $t_C = \lfloor (d_C - 1)/2 \rfloor$ and denote the covering radius of C by r_C.

Proof
See Helleseth et al. [7, Lemma 2]. This property is due to the fact that the sets of correctable and uncorrectable errors form a monotone structure, (see, for example, [10, p. 58, Theorem 3.11]) and a result of Bollobas about shadows [1, Theorem 3]

5.1 A corollary of Theorem 1

For Reed-Muller codes of order r, that is to say $RM(n, r)$ we take

$$t = 2^{n-1} - c\sqrt{2^{n-1}\binom{n}{r}\ln 2}.$$

Corollary 1 . *If $c > 1$, then $\epsilon_C(t_c) \to 1$ when $n \to \infty$.*

Proof.
We know that the ratio of the unambiguous correctable errors (hence also the correctable errors) of weight smaller than t_c to the words of weight smaller than t_c tends to 1 when n tends to infinity. We have to show that the ratio of the correctable errors of weight exactly t_c to the words of weight exactly t_c tends to 1 when n tends to infinity.
For an $RM(n, r)$ code, let

$$\frac{2^{2^n}}{\sqrt{\pi}} \frac{2^{-c^2\binom{n}{r}}}{2c\sqrt{\binom{n}{r}\log 2}} = A(c).$$

Let us fix c_1 and suppose that $\epsilon_C(t_{c_1}) \not\to 1$. Then there exists $\eta < 1$ such that $\epsilon_C(t_{c_1}) < \eta$ for an infinity of n. If $c_1 > c_2 > 1$, then among the words of weights between t_{c_1} and t_{c_2} there is only at most a proportion η of correctable words as the function ϵ_C decreases. From Proposition 3 there are about

$$\sum_{0 \le i \le \delta_1} \binom{2^n}{i} \;=\; A(c_1)(1+o(1)).$$

words of weight in $[0,\ t_{c_1}]$ and

$$\sum_{\delta_1 \le i \le \delta_2} \binom{2^n}{i} \;=\; A(c_2)(1+o(1)).$$

words of weight between t_{c_1} et t_{c_2}. As $A(c_1) = o(A(c_2))$ there are at most

$$A(c_1)(1+o(1)) + \eta A(c_2)(1+o(1)) = \eta A(c_2)(1+o(1))$$

correctable words of weights $[0,\ t_{c_1}]$, which shows that it is impossible that almost all words are correctable as says Theorem 1.

5.2 Proof of the Theorem 2. An asymptotic decoding upper bound

In the case of RM codes we have a simplification of the proof of the Theorem 3 b in [7].

Proposition 4 . *If* $c < 1$, *then* $\epsilon_C(t_c) \to 0$ *when* $n \to \infty$.

For every t, one has (cf. Lemma 3 of [7])

$$\begin{aligned}
\epsilon_C(t) \times \sum_{i=0}^{t} \binom{2^n}{i} &\le \sum_{i=0}^{t} \epsilon_C(i) \binom{2^n}{i} \\
&= \text{number of correctable errors of weight smaller than } t \\
&\le \text{total number of correctable errors} \\
&\le 2^{2^n-k}.
\end{aligned}$$

We have, from Proposition 3

$$\sum_{i=0}^{t_c} \binom{2^n}{i} \;=\; \#B_{t_c} = \frac{2^{2^n - c^2\binom{n}{r}}}{2c\sqrt{\pi \binom{n}{r} \ln 2}}(1+o(1)).$$

Whence

$$\begin{aligned}\epsilon_C(t_c) &\leq \frac{2^{2^n-k}}{\sum_{i=0}^{t_c}\binom{2^n}{i}} \\ &= \frac{2c\sqrt{\pi\binom{n}{r}\ln 2}}{2^{2^n-c^2\binom{n}{r}} \times 2^{\sum_{i=0}^{r}\binom{n}{i}-2^n}}(1+o(1)) \\ &= \frac{2c\sqrt{\pi\binom{n}{r}\ln 2}}{2^{\sum_{i=0}^{r}\binom{n}{i}-c^2\binom{n}{r}}}(1+o(1)).\end{aligned}$$

If $c < 1$, when $n \to \infty$ then the denominator tends toward infinity, so $\epsilon_C(t_c) \to 0$.

Remark.
This proposition is still true if we take $t_c = 2^{n-1} - c\sqrt{2^{n-1}k\ln 2}$ with $c < 1$ if $k \leq 2^{(n-1)/4}$ (to be able to use Proposition 3).

5.3 End of the proof of Theorem 2.

Remark that the statement of Theorem 2 does not involves ambiguously correctable errors. So we have the choice of ambiguous correctable errors, and we can choose the lexicographically smallest minimum-weight vectors as the coset leaders as in the beginning of the section 5.
Then one has from the last proposition

$$P_{wt(e)\geq\delta}\Big(e \text{ is correctable}\Big) \leq \epsilon(\delta) \to 0$$

when n tends to infinity. Therefore

$$P_{wt(e)\geq\delta}\Big(e \text{ is unambiguously correctable}\Big) \to 0$$

which means that Theorem 2 is true.

5.4 Asymptotically optimality of RM codes

A sequence $(C_m)_m$ of $[m,k]$ codes where $k = o(m)$ as $m \to \infty$ is called asymptotically optimal if for any fixed ϵ, $0 < \epsilon < 1$

$$m - 2t_{C_m}(\epsilon) \sim \sqrt{mk\ln 4}$$

where the error correction capability function $t_C(\epsilon)$ is the maximum t such that $\epsilon_C(t) \geq \epsilon$.

Theorem 3 . *The sequence $RM(n,r)_n$ is asymptotically optimal.*

Proof.
Let us take ϵ and try to find $t_C(\epsilon)$.
Let $c < 1$.
If $2t_c = 2^n - c\sqrt{2^n k \log 4}$ then the words of weight t_c are almost all uncorrectable, therefore $\epsilon_{C_{2^n}}(t_c) \to 0$ as $n \to \infty$. And we have $\epsilon_{C_{2^n}}(t_c) < \epsilon$ for n big enough (and consequently $t_c \geq t_{C_{2^n}}(\epsilon)$).
As a result $t_{C_{2^n}}(\epsilon) \leq 2^{n-1} - c\sqrt{2^{n-1} k \log 4}$.

Let now $c > 1$.
If $2t_c = 2^n - c\sqrt{2^n k \log 4}$ then the words of weight t_c are almost all correctable, therefore $\epsilon_{C_{2^n}}(t_c) \to 1$ as $n \to \infty$. And we have $\epsilon_{C_{2^n}}(t_c) > \epsilon$ for n big enough (and consequently $t_c < t_{C_{2^n}}(\epsilon)$).
As a result, if $c_1 < 1 < c_2$, one has

$$2^n - c_2\sqrt{2^n k \log 4} < 2t_{C_{2^n}}(\epsilon) < 2^n - c_1\sqrt{2^n k \log 4}$$

or

$$c_1\sqrt{2^n k \log 4} < 2^n - 2t_{C_{2^n}}(\epsilon) < c_2\sqrt{2^n k \log 4}$$

or

$$c_1 < \frac{2^n - 2t_{C_{2^n}}(\epsilon)}{\sqrt{2^n k \log 4}} < c_2.$$

As c_1 and c_2 may be as close to 1 as we wish, we have

$$\frac{2^n - 2t_{C_{2^n}}(\epsilon)}{\sqrt{2^n k \log 4}} \to 1 \quad \text{when} \quad n \to \infty.$$

References

[1] B. Bollobas: Combinatorics: Set Systems, Hypergraphs, Families of Vectors, and Combinatorial Probability. Cambridge, U.K.: Cambridge Univ. Press, 1986.

[2] C. Carlet: The complexity of boolean functions from cryptographic viewpoint. In Matthias Krause, Pavel Pudlàk, Rüdiger Reischuk, and Dieter van Melkebeek, editors, Complexity of Boolean Functions, volume 06111 of Dagstuhl Seminar Proceedings. Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI), Schloss Dagstuhl, Germany, 2006.

[3] S. Dib: Distribution of boolean functions according to the second-order nonlinearity. In M. Anwar Hasan and Tor Helleseth, editors, WAIFI, volume 6087 of Lecture Notes in Computer Science, pages 8696. Springer, 2010.

[4] S. Dib: Thèse. Distribution de la non-linéarité des fonctions Booléennes. Université d'Aix-Marseille, 2013.

[5] W. Feller: An introduction to probability theory and its applications. Vol. I. Third edition. John Wiley & Sons Inc., New York, 1968.

[6] R. L. Graham, D. E. Knuth, and O. Patashnik: Concrete mathematics. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1989. A foundation for computer science.

[7] T. Helleseth, T. Kløve, and Vladimir I. Levenshtein: Error correction capability of binary linear codes. IEEE Trans. Inform. Theory, 51(4):14081423, 2005.

[8] T. Kaufman, S. Lovett, E. Porat: Weight distribution and list-decoding size of Reed-Muller codes. IEEE Trans. Inform. Theory 58 (2012), no. 5, 26892696.

[9] S. Litsyn and A. Shpunt:. On the distribution of Boolean function nonlinearity. SIAM J. Discrete Math., 23(1):79 95, 2008/09.

[10] W. W. Peterson and E. J. Weldon Jr. Error-Correcting Codes. Cambridge, MA: MIT Press, 1972.

[11] F. Rodier: Sur la non-linéarité des fonctions booléennes, Acta Arithmetica, vol 115, (2004), 1-22, ArXiv : math.NT/0306395.

[12] F. Rodier: Asymptotic nonlinearity of Boolean functions, Designs, Codes and Cryptography, 40 :1 2006.

[13] K. U. Schmidt: Nonlinearity measures of random Boolean functions, preprint, 2013, arXiv:1308.3112.